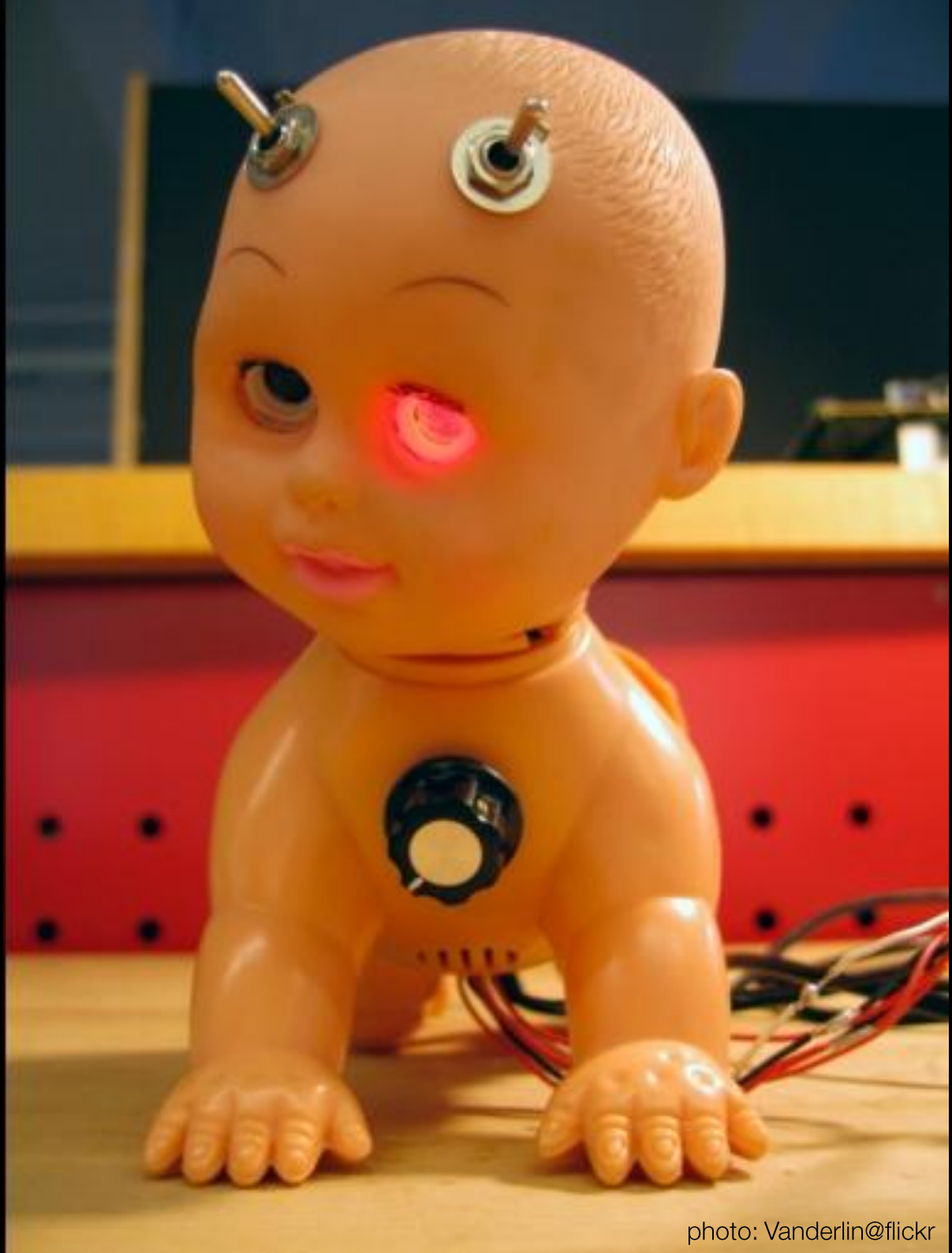


Hacking my
children's
toys...



Why do this?

Because you can.

You can do something with a product or a piece of hardware that has never been done before.

You can create something extraordinary.

You harm nobody in the process.

- Joe Grand

Under the knife today...



Leapster Explorer (aka LX)



Didj



Feeds and Speeds:

LF1000 (aka Pollux)
ARM 926EJ-S – 393MHz

32 (Didj) or 64MB (LX) SDRAM
256 (Didj) or 512MB (LX) NAND



USB Host
(LX – via Accessory port)
USB Device
(Didj/LX)

Research: Get datasheets.

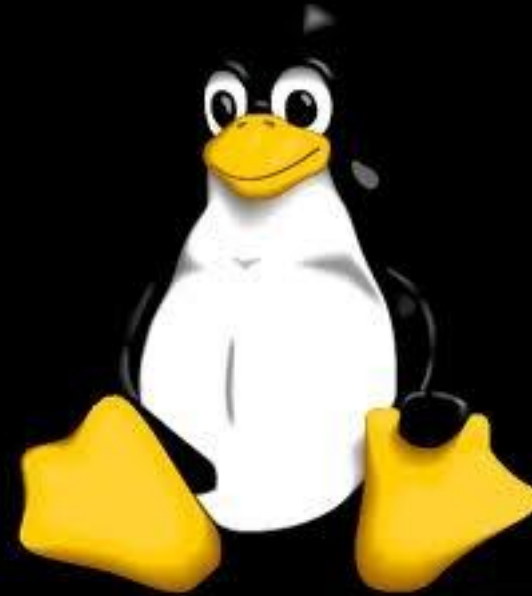
Key facets of the LF1000 CPU as revealed in the datasheets:



1. Embedded Serial I/O (UART)
2. Ability to boot from UART
3. Onboard USB, I2C, SPI
4. Composite TV Out***

Get the datasheets.
(Google is your friend!)





Research: Get source.

Next,investigate the interfaces:

Look for ways in...

Tools:

Multimeter

Soldering Iron (be not afraid!)

A few electronic components

...and your powers of observation.

Ways in...

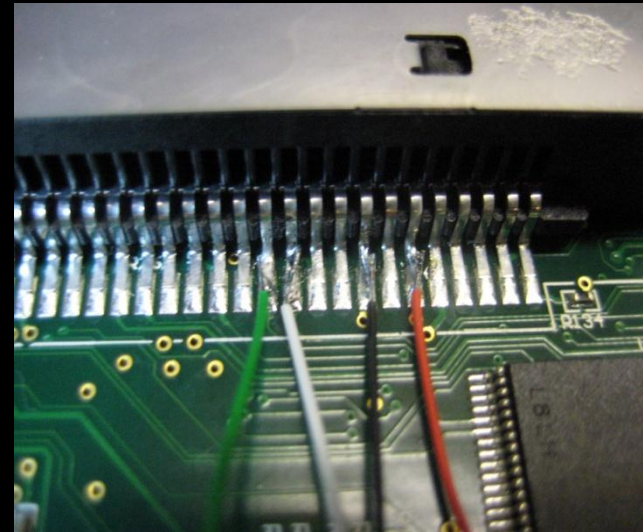
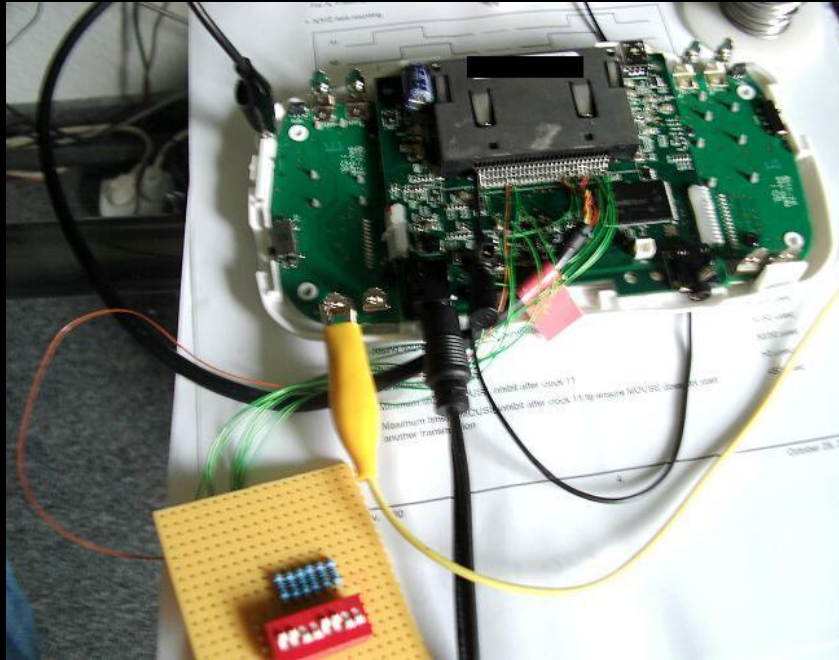
Cartridge Socket

USB

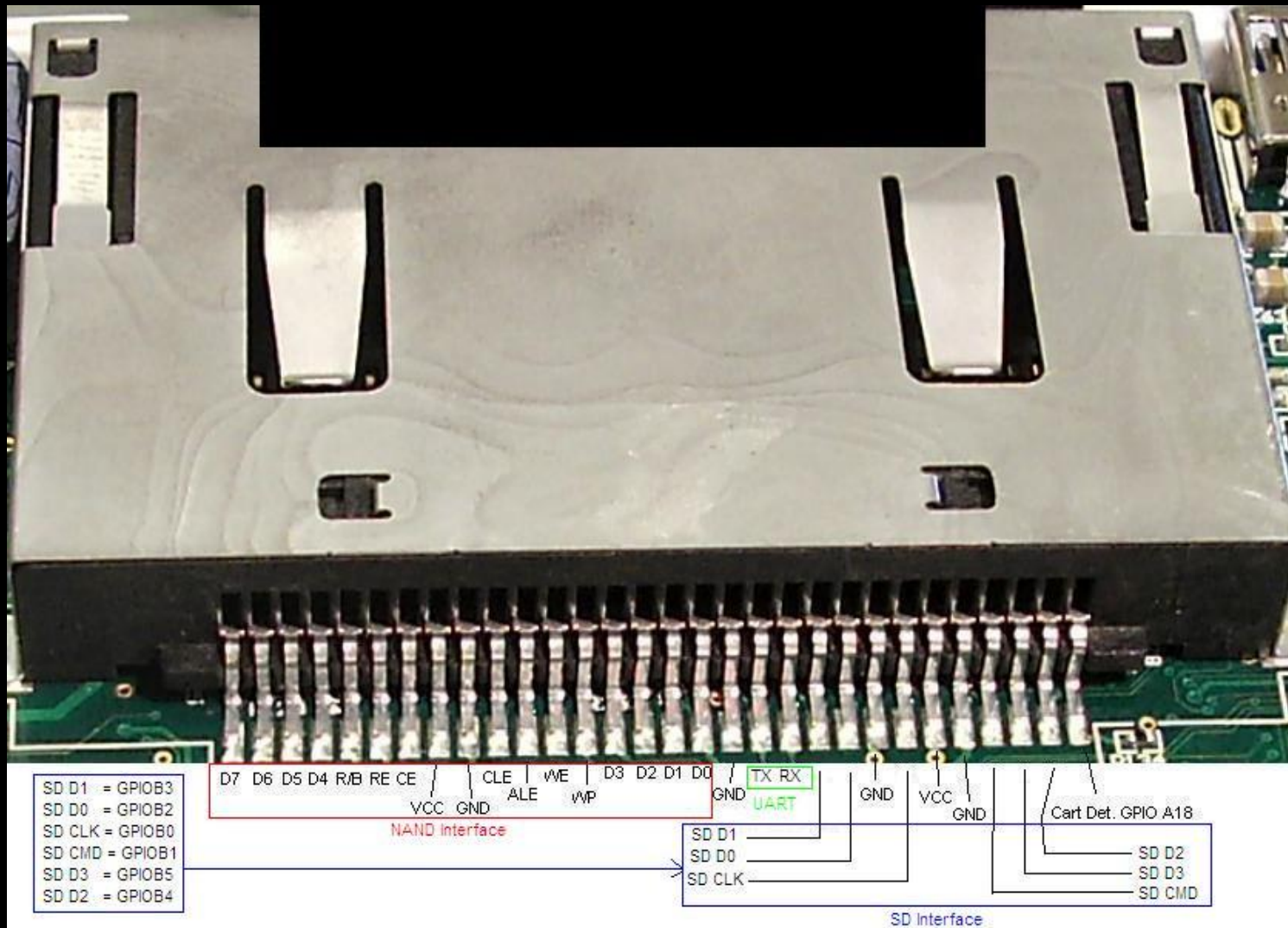


Ways in:

The Cart Socket...

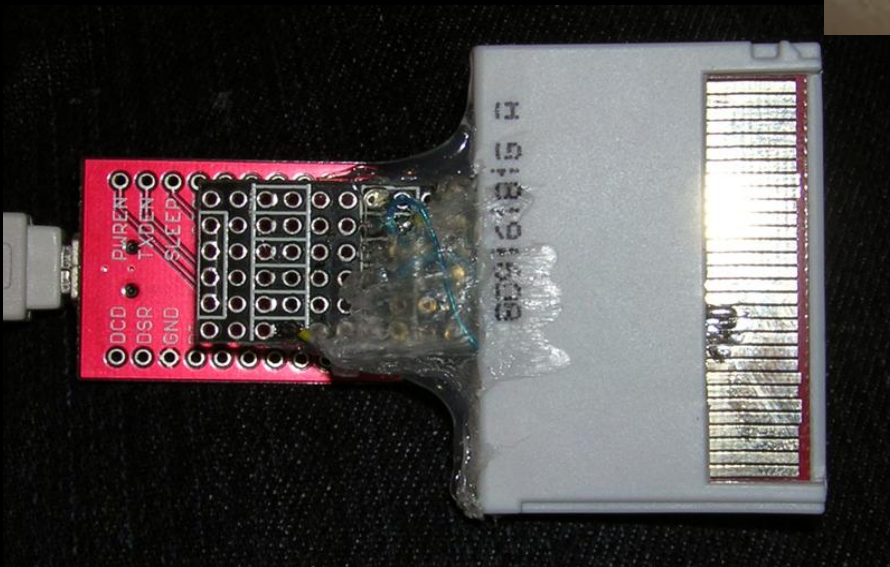
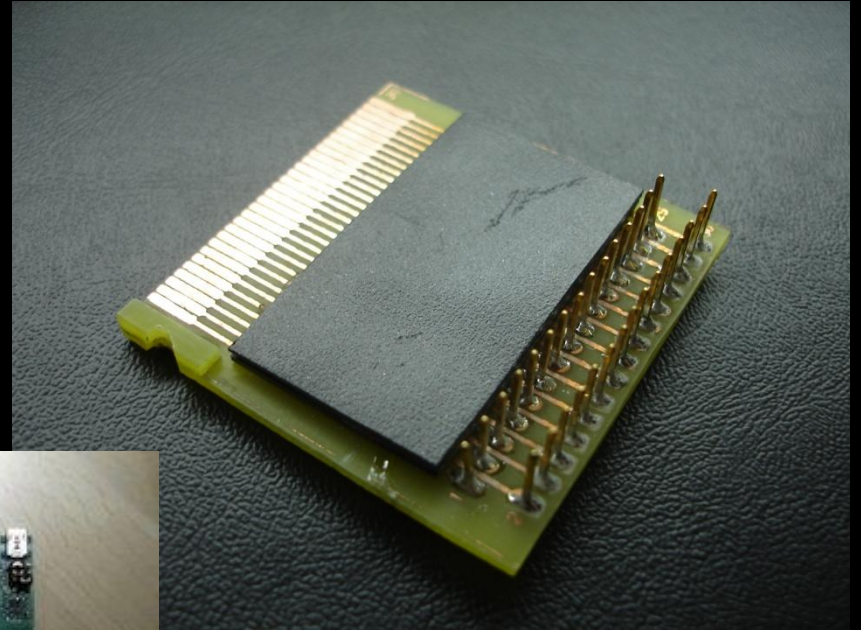


Bingo! 115200 8N1 (yay!)

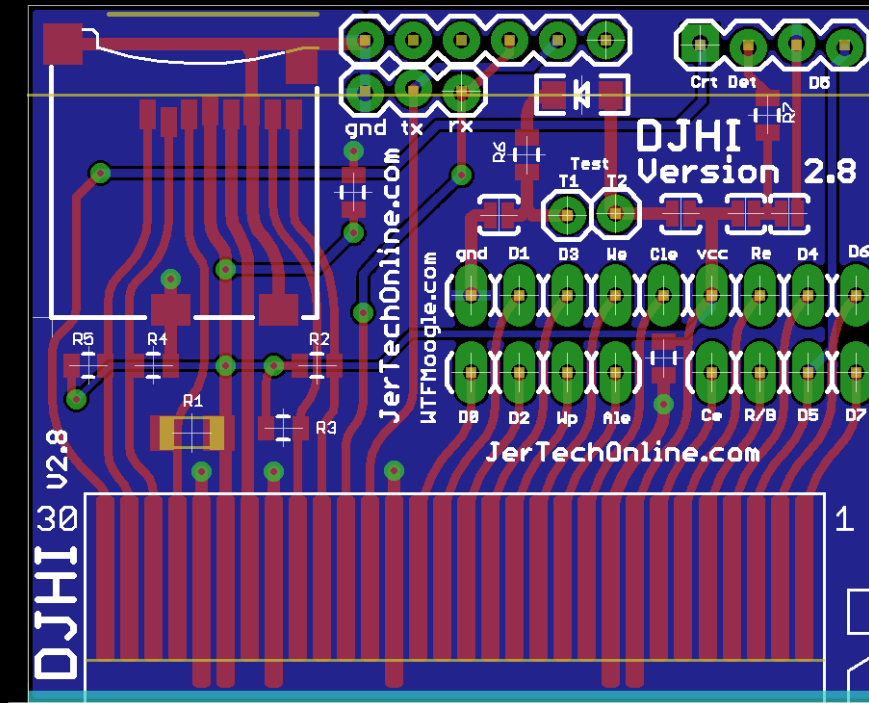


What was found? Serial, SDIO, NAND (ex. xD)

A rogue's gallery of homebrew
breakout boards:



The first hacker-developed product, the DJHI*:



**DidJa Hack It?*

Demo: Got Root? (on a toy!)

Demo: Taking control...UART Boot.
(Remember the datasheet?)

Deeper investigation: Reversing the hardware.

Tools:

Flatbed scanner

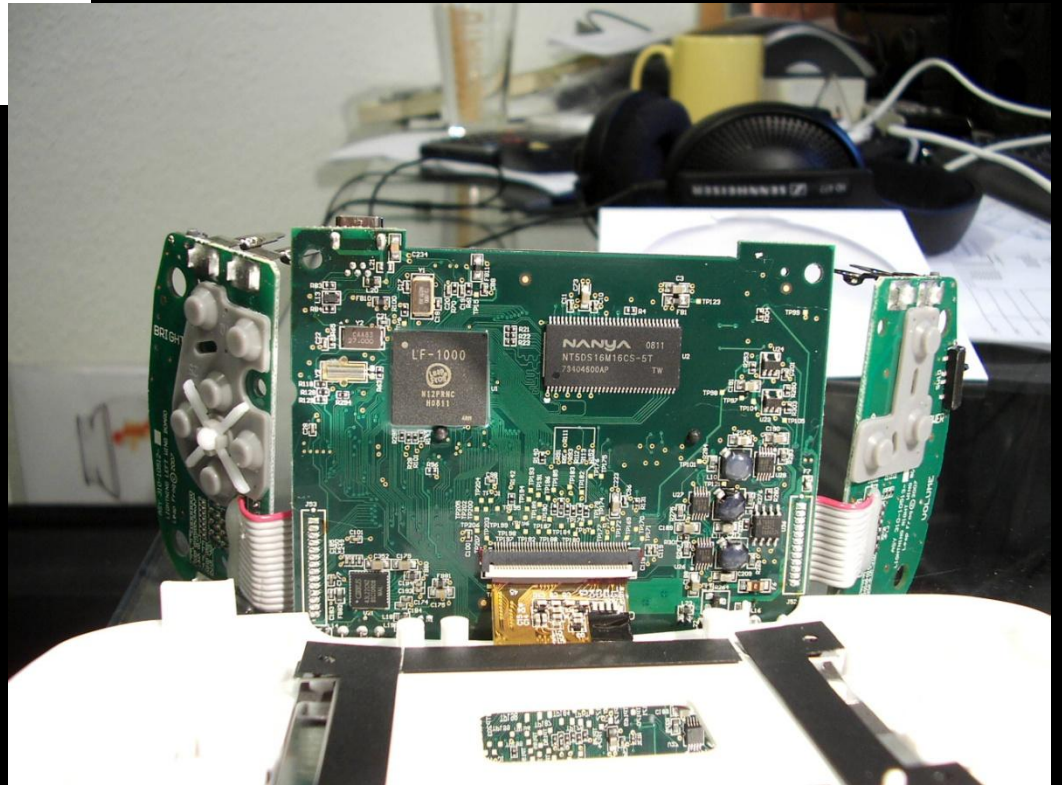
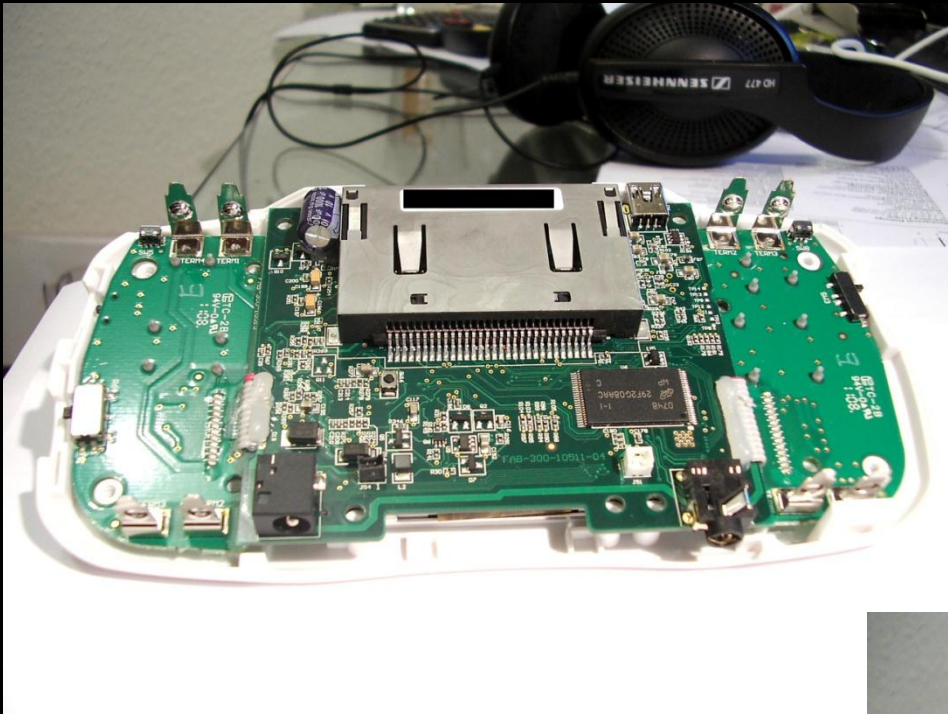
Stereo microscope (or a USB microscope.)

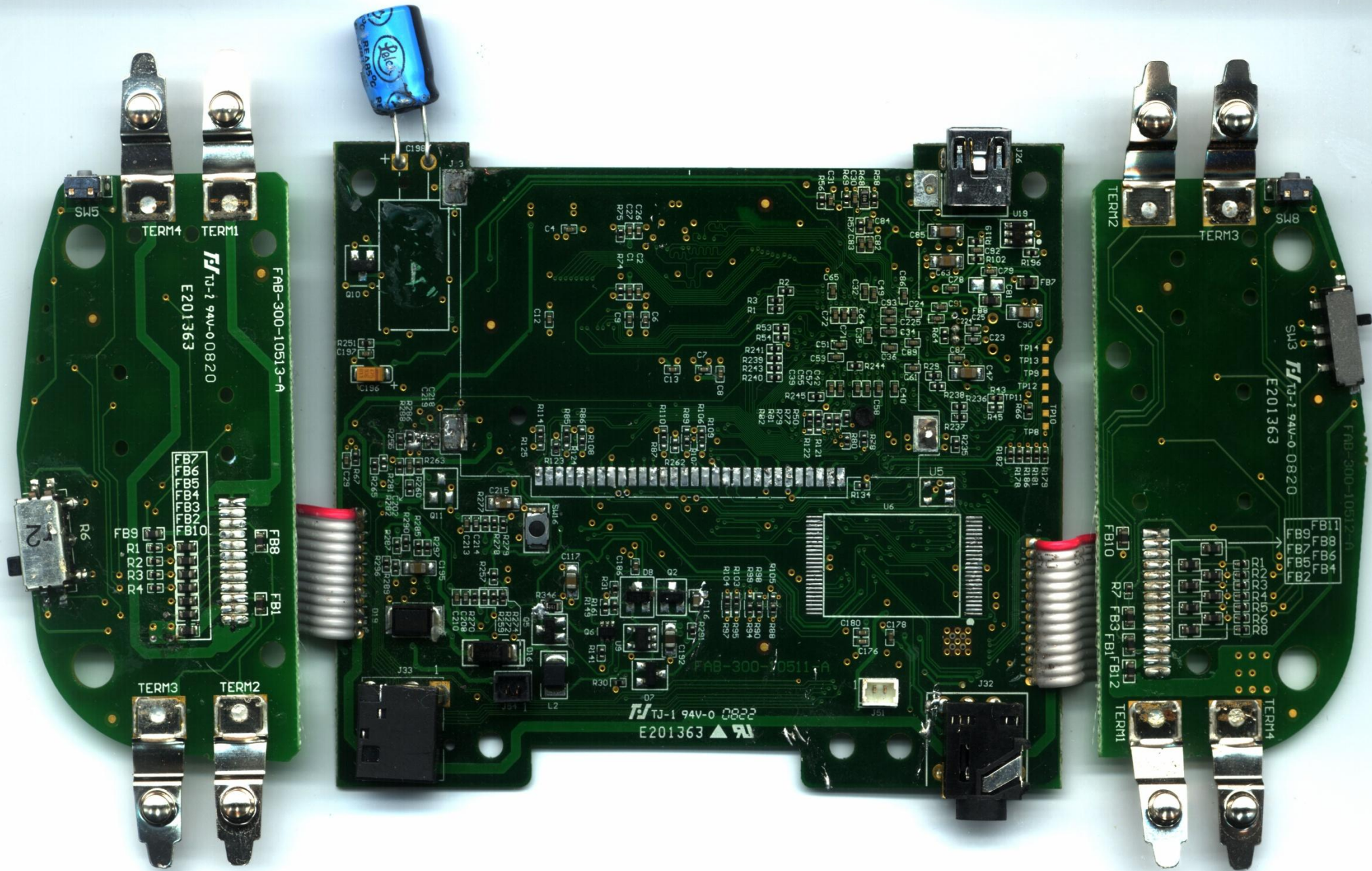
Heatgun (or a hot-air SMD rework station)

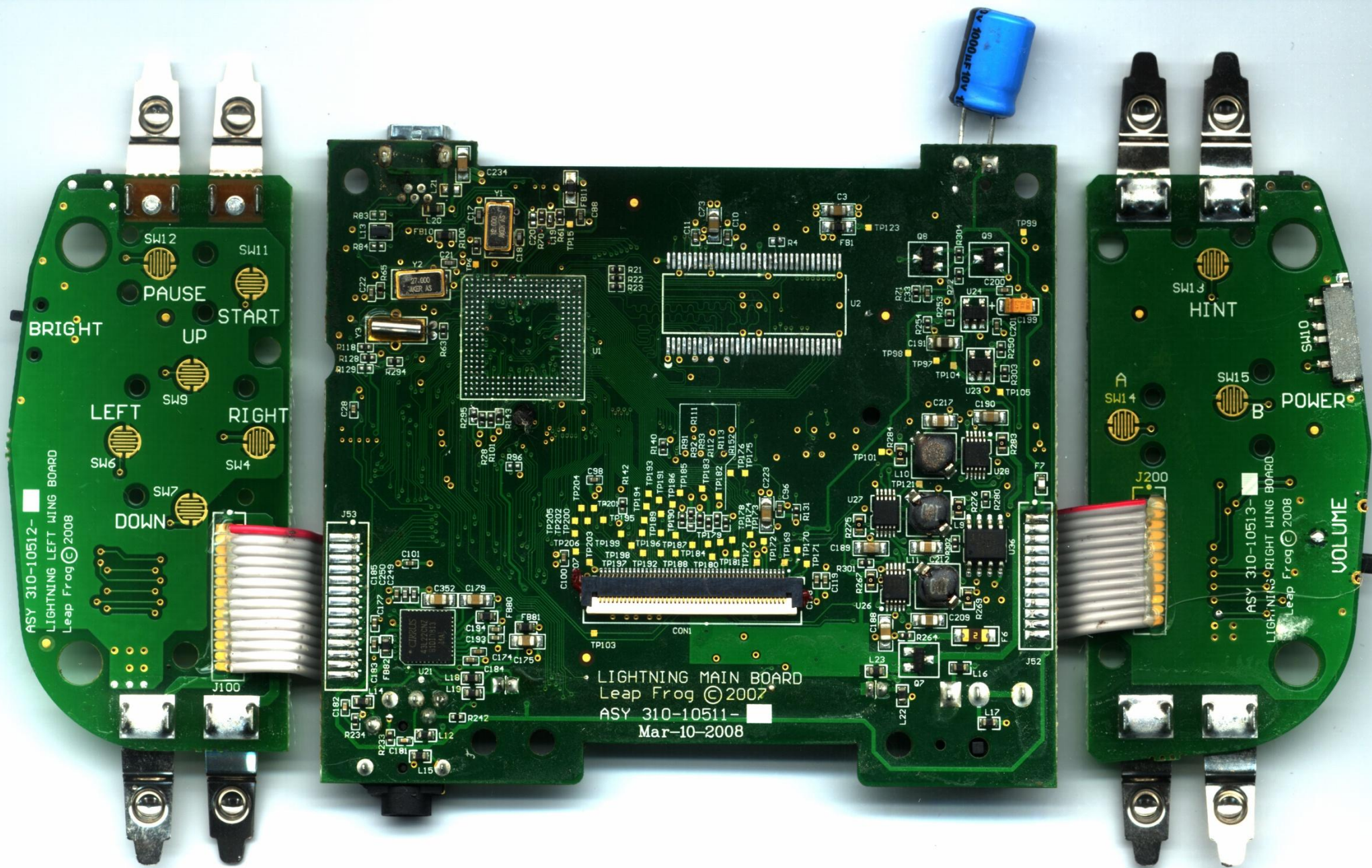
Multimeter

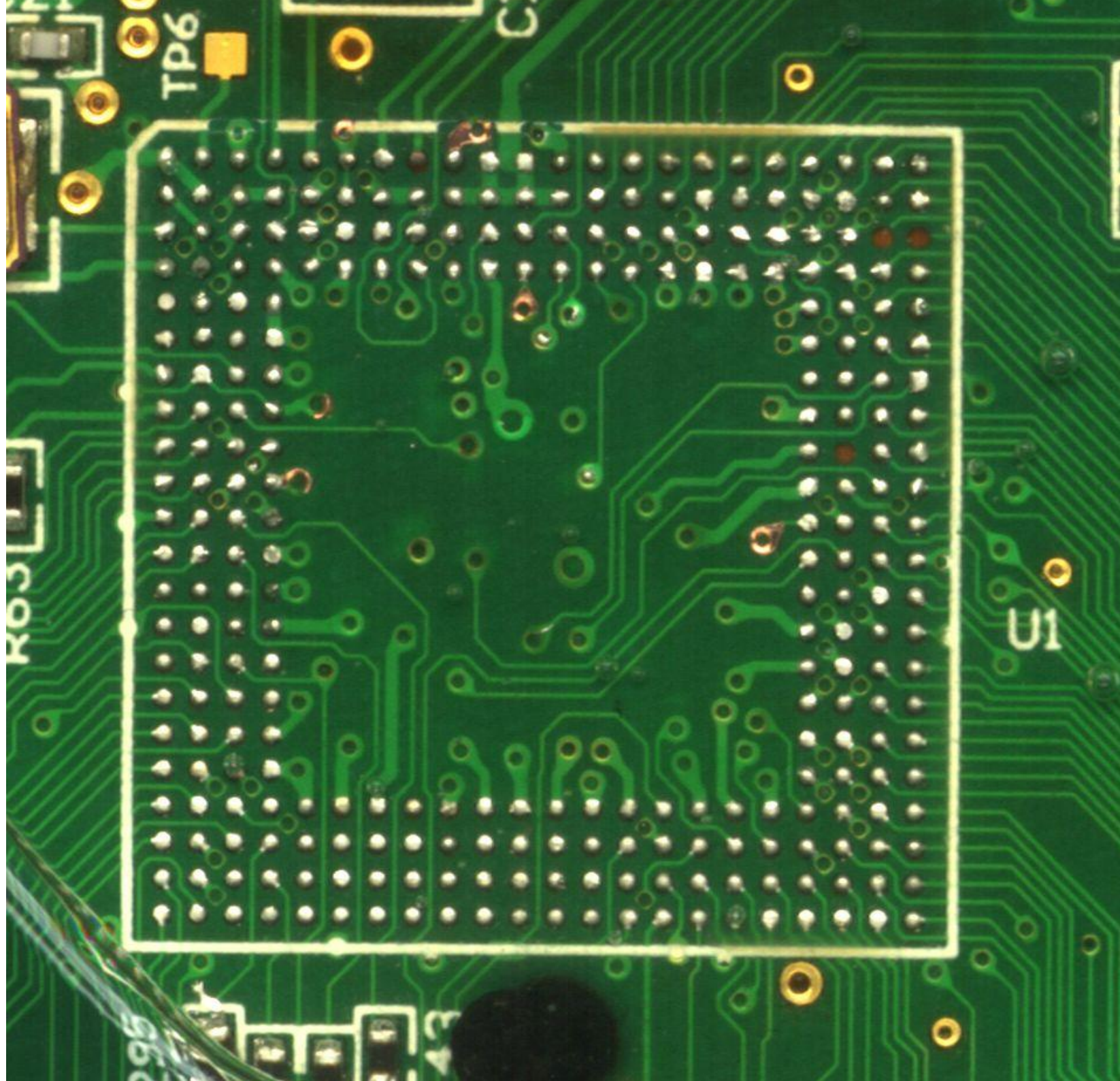
JTAG dongle

Datasheet

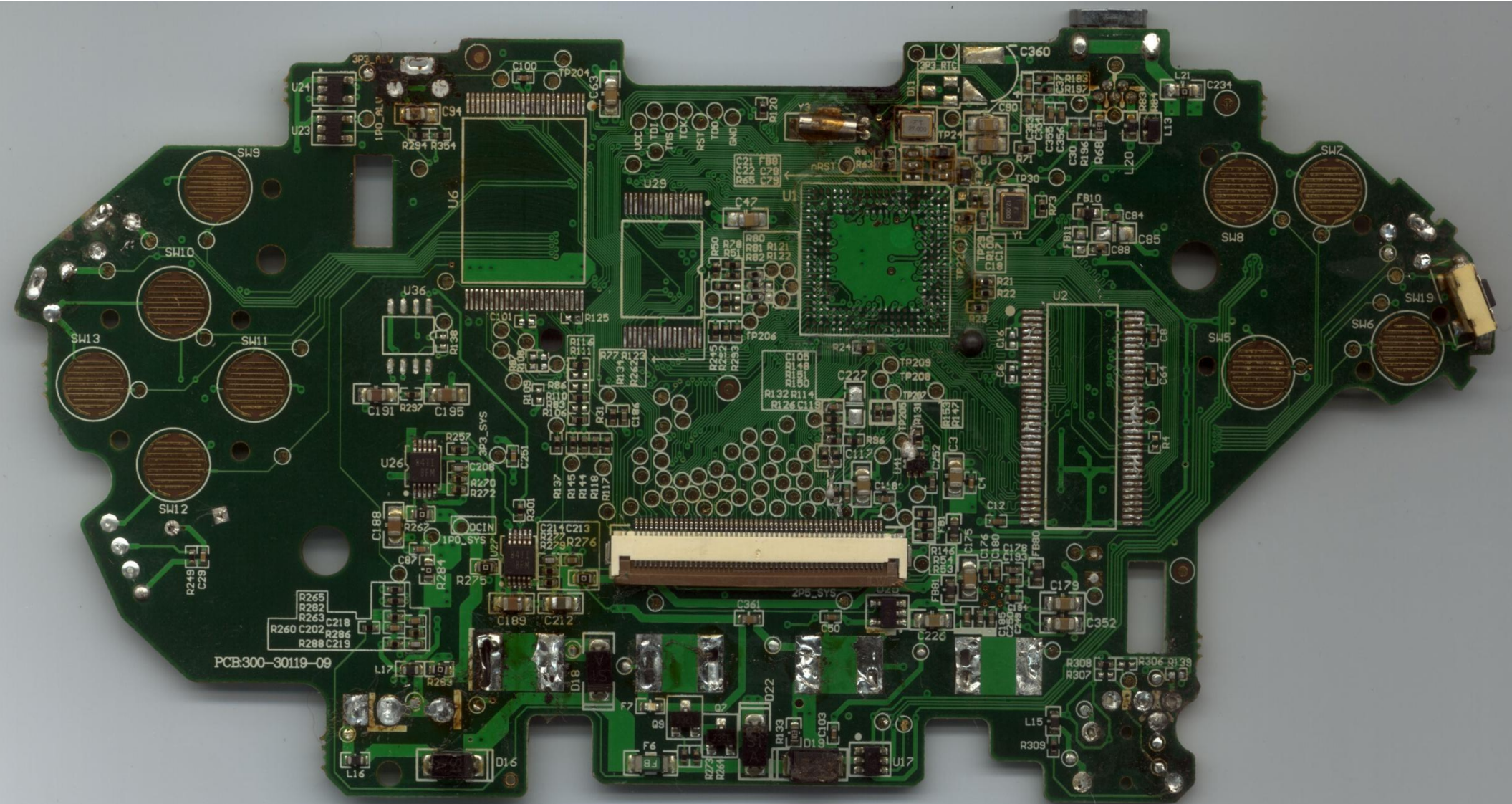








	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	
A	VDD10A_P LL0	VIDEO	VDD33A_L DAC	USBX1	USBX0	VSS33A_L USB2C	USBDP	USBDM	VSS33A_L USB2A	ADCIN6	VDD33A_L ADC	VSS33A_L DC	YA4	YA6	YA8	YA11	YDQM1	YCK	YCKE	YD7	YD5	YD4	A
B	VSS10A_P LL0	VDD10A_P LL1	VSS33A_L AC	VSSA33C USB2	VDDA33C _USB2	VSS33A_L USB2B	VDD33A_L USB2B	VDD33A_L USB2A	ADCIN4	ADCIN5	ADCIN7	ADCREF	YA5	YA7	YA9	YA12	YhCK	YDQM0	YDQS0	YD6	YD3	YD2	B
C	XTI	VSS10A_P LL1	VREF	IREF	USBTEST A	UP	UM	ADCIN2	ADCIN3	VDD33D _ADC	YD15	YD13	YD12	YD11	YD10	YD8	YhWE	YhCAS	YhRAS	YhCS0	YD1	YD0	C
D	XTO	GPIOLIV E1	VCOMP	VSS33A_L DAC	USBREXT	USBVBUS	ADCIN0	ADCIN1	VSS	VDDI10	YD14	YD9	YDQS1	YhF	VSS25	VDD25	VSS25	VDD25	VSS25	YBA0	YA10	YA0	D
E	GPIOLIV E3	GPIOLIV E2	GPIOLIV E0	VDD33A_L DAC															VDD25	YBA1	YA1	YA2	E
F	GPIOLIV E6	GPIOLIV E5	GPIOLIV E4	VDD33D _DAC															VDD25	SDDAT12	SDDAT12	YA3	F
G	XTIRTC	VDD_RTC	PORSEL	VDDI10_A LV															SDDAT11	SDDAT10	SDDAT03	SDDAT02	G
H	XTQRTC	VDDPWRO N	hBATF	VDD33_A LV															VSS	SDCMD1	SDDAT01	SDDAT00	H
J	TDO	TCK	VDDPWR TOGGLE	VSS															VDDI10	SDCLK1	SDCMD0	SDCLK0	J
K	TMS	TDI	hTRST	VDDI10															VSS	SDA1	SCL1	SDA0	K
L	RK0	hPORST	ITAGMOD E	VSS															VDD33_IC	SSPFRM0	SSPRXD0	SCL0	L
M	TX0	hEXTRST	TEST_EN	VDD33_IC															SSPFRM1	SSPCLK1	SSPTXD0	SSPCLK0	M
N	TX1	hCTS1	hRTS1	VSS															SSPRXD1	SSPTXD1	PVSYNC(Y D)	PVCLK	N
P	RK1	hRIO1	hDCD1	VDDI10															VSS	PVD12	PDE(CL2)	PHSYNCL QL1	P
R	TX2	RK2	TX3	hDSR1															VDD33_IC	PVD13	PVD1	PVD0	R
T	PWMOUT0	PWMOUT1	RK3	hDTR1															PVD14	PVD15	PVD3	PVD2	T
U	2SDAT0	2SSYNC	PWMOUT2	VDD33_IC															PVD16	PVD17	PVD5	PVD4	U
V	2SMCLK	2SSCLK	2SDAT1	VSS															PVD19	PVD18	PVD7	PVD6	V
W	SA23	SA24	SA25	NC	VSS	VDDI10	VSS	hSCS4	VDD33_IC	VSS	VDDI10	VSS	VDD33_IC	VSS	RnB	VSS	VDD33_IC	VDDI10	VSS	PVD20	PVD9	PVD8	W
Y	SA21	SA22	hSCS9	NC	RDnWR	hSCS6	hSCS5	hSCS3	hSCS2	hSCS1	hSCS0	hSOE	hSWE	hNCS1	hNFOE	hNCS0	NPCLEI	NFALE	hNFIWE	PVD23	PVD11	PVD10	Y
AA	SA20	hSCS8	LATADDR	hSWAIT	SA17	SA15	SA13	SA11	SA9	SA7	SA5	SA3	SA1	SD15	SD13	SD11	SD9	SD7	SD5	SD3	PVD22	PVD21	AA
AB	SA19	hSCS7	hSDQM1	SA18	SA16	SA14	SA12	SA10	SA8	SA6	SA4	SA2	SA0	SD14	SD12	SD10	SD8	SD6	SD4	SD2	SD1	SD0	AB
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	



Discoveries: TV, SPI, JTAG, Audio...

Deeper investigation: Use the Source!

Development:

Tools: Source code. IDE. Cross compiler.

Development:
Framebuffer device
SDL

Demo: Combining what we learned. TV, Emu

Methods Recap:

- Get Datasheets

- Get Source

- Look for ways in.

- Reverse the hardware.

- Use the source.

Tools Recap:

- Multimeter

- Oscilloscope – nice to have.

- Soldering Iron (really, its easy)

- Hookup wire

- Basic electronics

- Heatgun

- Brain (one or more)

elinux.org/Didj
elinux.org/Leapster_Explorer

rosincore.com
[irc.freenode.org #Didj](https://irc.freenode.org/#Didj)
nick: nirvous
hackaday.com/?s=nirvous